Sailors assigned to Navy Cyber Defense Operations Command (NCDOC) monitor, analyze, detect and respond to unauthorized activity within U.S. Navy information systems and computer networks. NCDOC is responsible for around the clock protection of the Navy's computer networks, with more than 700,000 users worldwide. (U.S. Navy photo by Mass Communication Specialist 2nd Class Joshua J. Wahl)

Cyber Law: Challenges, Law, and Billets

By Cmdr. Doug Velvel,
Intelligence Operations & Cyber Law Division (Code 18)

How to legally conduct military operations in cyber space has proven to be an enormous challenge. Even the most fundamental issue of law - what body of law applies to cyber space operations – has been debated. Despite the ongoing dialogue among legal scholars and policy makers on the applicable legal structure to apply, cyber threats to U.S. national security or interests continue to mount. The threats are so pervasive, insidious, and full of complex nuances that the nation's long-term health and welfare sometimes requires immediate actions despite the murky water that is cyber law and policy. It is in this perplexing, unresolved, and increasingly crucial operational environment that a Navy judge advocate must operate.

In today's operational environment, cyber operations are seldom stand alone operations from traditional air, land, and sea operations. Cyber operations have become mainstream parts of most military strategies, fully integrated into operational plans and missions.

Capt. Stu Belt, Director of OJAG's International and Operational law Division, described his recent experience as the Fleet Judge Advocate for Commander, U.S. Pacific Fleet: "For all of our high end war plans in the Pacific, cyber capabilities were always a critical part of the planning process. It became more clear during my tour that I needed operational law JAGs who could not only provide legal advice in the more traditional areas of air and sea operations, but who could also identify the salient issues related to cyber targeting and authorities in any given operation." But what are those issues?

The Body of Law

The starting point is the Law of Armed Conflict (LOAC). Though there are no international treaties or agreements directly on point that regulate military operations in cyber space, in 2011 the U.S. identified its legal position in its "International Strategy for Cyberspace." Specifically,

Cyber continued on page 24

Cyber continued from page 23

the U.S. stated that "[t]he development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them."

Cyber operations have become mainstream parts of most military strategies, fully integrated into operational plans and missions.

While this U.S. position may be a beginning point in the creation of customary international law recognizing the application of the LOAC to military operations in cyber space, the custom and practice of States is still developing. In a September 2012 speech, the State Department Legal Advisor, Mr. Harold Koh, reiterated that "the United States has made clear our view that established principles of international law do apply in cyberspace….in the context of an armed conflict, the law of armed conflict applies to regulate the use of cyber tools in hostilities, just as it does other tools…." He further stated that the "unique attributes of networked technology require additional work to clarify how these norms apply."

A Horde of Uncertain Legal Issues

The challenge, of course, lies in addressing the "unique attributes." Most of the legal challenges of cyber operations are linked to the application of the LOAC. Examples include, inter alia: How can one comply with the core LOAC requirement of distinction if cyber effects cannot be sufficiently attributed, or….perhaps the cyber action is being executed via a server in a third state, putting that state's sovereignty at issue, or…. while self-defense is always available against an armed attack, what constitutes an armed attack in cyber space? In his recent speech, Mr. Koh provided the U.S. position that "cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force" equating to an armed attack. The level of destruction required to be a "use of force" or "armed attack" is still a matter of active debate.

Cyber Law Opportunities

An oft-asked question is "how do I get into cyber law?" The answer is simple - pursue whatever operational law billet is available.

Within the Navy, the only dedicated operational cyber billets are at Fleet Cyber Command/10th Fleet. Navy billets in joint commands/offices that are cyber-specific in nature include CYBERCOM, the National Security Agency and the office of the DoD Deputy General Counsel (Intelligence). The work done by Navy judge advocates at each of these commands/offices is highly classified, meaning little can be discussed here. But the judge advocates at these commands are at the cutting edge of our national defense, supporting operations with some of the most exciting and sophisticated national security legal work in the military. But as exemplified by Belt's experience, any operational command, whether joint like a Combatant Command or service-specific like Pacific Fleet, either has or will soon have a significant cyber operational element. The judge advocate who is prepared to handle the spectrum of operational legal issues will be the one to whom the commander turns.